Aula 10

O CONCEITO DE ANEL

META

Apresentar o conceito de anel, suas primeiras definições, diversos exemplos e resultados.

OBJETIVOS

Definir, exemplificar e classificar anéis.

Aplicar as propriedades dos anéis na relação de problemas.

Reconhecer subanéis.

PRÉ-REQUISITOS

O curso de Fundamentos de Matemática e as aulas anteriores.

INTRODUÇÃO

Os números inteiros, racionais, reais e complexos podem ser somados e multiplicados entre si, e o resultado é ainda um número do mesmo conjunto. Analogamente, podemos somar e multiplicar matrizes de mesma ordem e outros tipos de objetos que são hoje bastante utilizados. Estes são exemplos de estrutura algébricas menos gerais que os grupos, pois, envolvem duas operações verificando um conjunto de operações similares, que são os ingredientes que compõem a definição da estrutura algébrica chamada anel.

Nesta aula estabeleceremos o conceito de anel, apresentando as primeiras definições, fazendo a classificação, exemplificando e estabelecendo as primeiras proposições sobre anéis.Vamos em frente.

O CONCEITO DE ANEL

Sejam A um conjunto não vazio, e, $+$: A x A ⟶ A e $\cdot$: A x $A \longrightarrow A$

$$(a,b) \rightsquigarrow a+b \quad (a,b) \rightsquigarrow a.b$$

duas operações em A.

Definição 1. Dizemos que $(A,+,\cdot)$ é um anel, se valem as propriedades:

i) $(A,+)$ é grupo abeliano. Ou seja,

1) $\forall a,b,c \in A,\ (a+b)+c = a+(b+c)$

2) $\exists 0 \in A;\ \ a+0 = 0+a = a$

3) $\forall a \in A,\ \exists -a \in A; a+(-a) = (-a)+a = 0$

4) $\forall a,b, \in A,\ \ a+b = b+a.$

ii) A operação $\cdot$ é associativa: $\forall a,b,c\ \in A,\ \ (a.b).c = a.(b.c)$

iii) Valem as leis distributivas: $\forall a,b,c \in A,$

1) $a.(b+c) = a.b + a.c$
2) $(a+b).c = a.c + b.c$

Exemplo 1. Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ munidos das suas operações de adição e multiplicação são exemplos de anéis.

Exemplo 2. O conjunto $A = M_2(\mathbb{Z})$ dos matrizes quadradas de ordem $\mathbb{Z}$ com nas operações tradicionais de adição e multiplicação é um exemplo de anel.

Se, num anel $(A,+,\cdot)$ vale a propriedade

iv) comutatividade da multiplicação: $\forall a,b \in A,\ \ a.b = b.a,$

dizemos que $(a,+,\cdot)$ é um anel comutativo.

Exemplo 3. Os termos $(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$ são exemplos de anéis comutativas. O anel $(M_2(\mathbb{Z}),+,\cdot)$ é um exemplo de anel que não é comutativo.

Se, num anel $(A,+,\cdot)$ vale a propriedade:

v) $\exists 1 \in A$ tal que $a.1 = 1,a = a\ \ \forall a \in A$, dizemos que $(A,+,\cdot)$ é um anel com identidade. Neste caso, 1 é a identidade do anel A.

Exemplo 4. Todos os anéis exibidos nos exemplos anteriores são anéis com identidade. Sejam $a \in \{2,3,4,\dots\}$ e $A = \{0,\pm a,\pm 2a,\dots\} \subset \mathbb{Z}$. É fácil ver que a soma e o produto de dois elementos de A são elementos de A. Segue que $(A,+,\cdot)$. Onde $+$ e $\cdot$ são as restrições das operações de adição e multiplicação de $\mathbb{Z}$, a A, é um anel sem elemento identidade.

Observação. Como em grupos, com o intuito de simplificar notação, costumamos escrever A em vez de $(A,+,\cdot)$ para representar tal anel.

Definição 2. Seja A um anel. Dizemos que o elemento $a \in A\backslash\{0\}$ é um divisor de zero, se existe $b \in A-\{0\}$ tal que $a.b = 0$.

Exemplo 5. Lembremos que para $n \in \{1,2,\dots\}$ na aula 3, nós afirmamos que $\mathbb{Z}_n = \{\overline{0},\overline{1},\dots,\overline{n-1}\}$ junto com as duas operações de adição e multiplicação ali exibidos tinha uma estrutura de anel. Notemos que de fato $(\mathbb{Z}_n,+,\cdot)$ é um exemplo de anel comutativo com elemento identidade $\overline{1}$, finito, com n elementos ($\mathbb{Z}_n$ é um anel que tem ordem n). Notemos que quando $n > 2$ não é primo, existem $n_1,n_2 \in \mathbb{Z},\ 2 \leq n_1,n_2 < n$ tais que $n_1.n_2 = n$. Assim, em $\mathbb{Z}_n,\ \overline{n_1} \neq \overline{0},\ \overline{n_2} \neq \overline{0}$ e $\overline{n_1}.\overline{n_2} = \overline{n} = \overline{0}$. Ou seja, os elementos $\overline{n_1}$ e $\overline{n_2}$ são divisores de zero.

Se, A é um anel comutativo com identidade no qual vale a propriedade

v) Integridade: Se $a,b \in A$ e $a.b = 0$ então $a = 0$ ou $b = 0$, dizemos que A é um domínio (ou anel de identidade).

Exemplo 6. Os anéis $\mathbb{Z},\mathbb{Q},\mathbb{R}$ e $\mathbb{C}$ são exemplos de domínios. Note que num domínio não há divisores de zero. Os anéis $\mathbb{Z}_n$ onde n não é primo não são domínios.

Exemplo 7. No anel $A = M_2(\mathbb{Z})$ os elementos $a = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$ e $b = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ são divisores de zero pois $a.b = 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Definição 3. Sejam A um anel com identidade e $a \in A$. Dizemos que a é invertível se existe um $b \in A$ tal que $a.b = b.a = 1$ indicamos o inverso de a por a^{-1}.

Exemplo 8. No anel $A = M_2(\mathbb{Z})$, o elemento $a = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ é invertível pois, $\exists b = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix} \in A$ tal que $a.b = b.a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{1}$.

Definição 4. Quando todos os elementos não nulos de um anel A são invertíveis, dizemos que A é um anel de divisão. Quando o anel de divisão é comutativo o chamamos de corpo.

Observação. Notemos que quando A é um anel de divisão, $(A\backslash\{0\},\cdot)$ é um grupo.

Indicamos o conjunto dos invertíveis de um anel A por A^* ou $\cup\,(A)$.

Exemplo 9. Os domínios $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos. O domínio $\mathbb{Z}$ não é um corpo, pois os únicos elementos invertíveis de $\mathbb{Z}$ são 1 e -1.

Proposição 1. (propriedades imediatas dos anéis) , seja A um anel.

i) O 0 (zero) é único.

ii) O oposto $-a$ de cada elemento a é único

iii) $\forall a \in A, a.0 = 0.a = 0$

iv) Se A tem identidade 1, esta é única.

v) $\forall a, b \in A, (-a).b = a(-b) = -(ab)$.

Demonstração. Deixaremos como atividade. Caro aluno, para desenvolver esta atividade, volte às aulas 1 e 4 e veja demonstrações semelhantes!

Exemplo 10. Anel nulo. Seja $A = \{0\}$ e definamos $0 + 0 = 0.0 = 0$. Então $(A, +, \cdot)$ tem estrutura de anel. O chamamos de anel nulo.

Proposição 2. Se A é um anel não nulo com identidade então $0 \neq 1$.

Demonstração. Se fosse $1 = 0$, então $\forall a \in A$, teríamos $a.1 = a.0 = 0$ e $A = \{0\}$.

Proposição 3. Num anel comutativo não nulo, um elemento não pode ser divisor de zero e invertível.

Demonstração. Sejam A um anel comutativo $a \in A$. Se a fosse divisor de zero e invertível, existiria um $b \in A\backslash\{0\}$ tal que $ab = 0 \Longrightarrow a^{-1}(ab) = a^{-1} \circ 0 \Longrightarrow b = 0$, uma contradição.

Proposição 4. Todo domínio finito é corpo.

Demonstração. Seja $A = \{a_1, \dots, a_n\}$ um domínio. Então dado $a \in A\backslash\{0\}$, $A = \{aa_1, \dots, aa_n\} = A$ pois se $aa_i = a_j$ temos $a(a_i - a_j) = 0$ com $a \neq 0 \Longrightarrow a_i = a_j$. Assim, como $1 \in A$, existe um $i \in \{1,2, \dots, n\}$ tal que $a.a_i = 1$, logo $a_i = a^{-1}$. Provamos então que todo elemento não nulo de A é invertível, ou seja, que A é um corpo.

Exemplo 11. Vamos apresentar aqui um anel de divisão que não é um corpo, ou seja, um anel de divisão no qual o grupo dos elementos invertíveis não é abeliano.

Seja $\mathbb{R}^4 = \{(a, b, c, d); a, b, c, d \in \mathbb{R}\}$ o conjunto de todos as 4-úplas de $\mathbb{R}$. Definimos a adição em $\mathbb{R}^4$, do seguinte modo: para $x = (a, b, c, d)$ e $y = (a', b', c', d')$, $x + y = (a + a', b + b', c + c', d + d')$ e, a multiplicação, $xy = (aa' - bb' - cc' - dd',\ ab' + ba' + cd' + c'd,\ ac' + a'c + db' - d'b,\ d' + da' + bc' - b'c)$.

Com algum trabalho, podemos verificar que $(\mathbb{R}^4, +, \cdot)$ tem estrutura de anel no qual o zero é $0 = (0,0,0,0)$.

Fazendo a identificação $a = (a, 0,0,0)$, $i = (0,1,0,0)$, $j = (0,0,1,0)$ e $k = (0,0,0,1)$, podemos escrever $x = (a, b, c, d) = a + bi + cj + dk$ de modo que podemos reescrever $\mathbb{R}^4 = \{(a + bi + cj + dk; a, b, c, d \in \mathbb{R}\}$

Neste anel valem:

$i^2 = j^2 = k^2 = -1,\ i.j = k,\ j.i = -k,\ j.k = i,\ k.j = -i,\ k.i = j$ e $i.k = -j$

Além disto,

$x + y = (a, b, c, d) + (a', b', ', d') = (a + a') + (b + b')i + (c + c')j + (d + d')k$ e $x.y = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' + ca' + db' - bd')j + (ad' + ba' + bc' - cb')k$. Este anel é conhecido como os quatérnios (ou quaterniões) é indicado por *Quat*, foi construído no século XIX, pelo matemático irlandês W. R. Hamilton quando tentava construir um corpo numérico que fosse uma extensão do corpo dos números complexos, sem sucesso. *Quat* só não é um corpo porque a multiplicação não é comutativa.

Observação. Com um pouco de trabalho, podemos verificar que o subconjunto $Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$ de Quat é fechado para a multiplicação. Mais ainda, $(Q_8, \cdot)$ tem estrutura de grupo.

Definição 5. Seja A um anel. Dizemos que um subconjunto não vazio B é um subanel de A, se sob as restrições das operações de adição e multiplicação a si, tem também estrutura de anel.

Uma condição necessária e suficiente para que um subconjunto não vazio B de um anel A seja um subanel é que cumpra às seguintes condições: $\forall a, b \in B,\ a - b \in B$ e $a.b \in B$. Com efeito, notemos que a condição: $\forall a, b \in B \Longrightarrow a - b \in B$ é necessária e suficiente para que $(B, +)$ seja um subgrupo de $(A, +)$. A condição: $\forall a, b \in B \Longrightarrow a.b \in B$ garante que B é fechado para a operação de multiplicação. Finalmente, como as outras propriedades de anel são válidas em A, valem a fortiori para B.

Exemplo 12. Para todo anel $A, \{0\}$ e A são subanéis.

Exemplo 13. Na seqüência de inclusões $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, cada anel é subanel dos que ficam à sua direita.

Exemplo 14. Para cada $a \in \mathbb{Z}$, o conjunto $a\mathbb{Z} = \{0, \pm a, \pm 2a, \dots\}$ munido das restrições das operações de adição e multiplicação dos inteiros é subanel de $\mathbb{Z}$.

Definição 6. Sejam A um anel comutativo e $n \in \mathbb{Z}$. Definimos

$$na = \begin{cases} 0\ , & se \quad n = 0 \\ a + (n-1)a, & se\ n > 0 \\ -\left((-n)a\right), & se\ \ n < 0 \end{cases}$$

Observação. Notemos que a definição acima nada mais é do que a de potência de expoente inteiro no grupo aditivo $(A, +)$, e, portanto para $a, b \in A$ e $m, n \in \mathbb{Z}$, valem:

i) $m(a + b) = ma + mb$

ii) $(m + n)a = ma + na$

iii) $(-m)a = -(ma) = m(-a)$

Definição 7. Seja A um anel comutativo não nulo definimos a característica de A como sendo o menor inteiro positivo n para o qual $na = 0, \forall a \in \mathbb{Z}$. Se não existe tal n dizemos que a característica de A é zero.

Exemplo 15. Nos anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, não existe inteiro positivo n tal que $na = 0$ para todo a no anel. Portanto estes anéis têm característica zero. Em $(\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}, +, \cdot)$ o menor inteiro positivo n para o qual $n\overline{a} = \overline{0},\ \forall \overline{a} \in \mathbb{Z}_n$ é $n = m$ logo, $\mathbb{Z}_m$ tem características m.

Definição 8. Dados um anel comutativo com identidade $A, a \in A$ e $n \in \mathbb{N}$, definimos:

$$a^n \begin{cases} 1\ se\ n = 0 \\ a.\,a^{n-1} se\ n > 0 \end{cases}$$

Valem e podem ser provadas

i) $a^m . a^n = a^{m+n}$

ii) $(a^m)^n = a^{mn}$ onde $a \in A$ e $m, n \in \mathbb{N}$.

Definição 9. Sejam A um anel comutativo com elemento identidade e $a \in A$. Dizemos que a é nilpotente se existe um $n \in \mathbb{N}\backslash\{0\}$ tal que $a^n = 0$

Exemplo 16. No anel $\mathbb{Z}_8, \overline{2}$ é nilpotente, pois $\overline{2}^3 = \overline{0}$.

Notamos que todo elemento nilpotente não nulo é um divisor de zero. Quando $a \in A$ é nilpotente, o menor inteiro positivo não nulo n para o qual $a^n = 0$ é chamado índice de nilpotência do elemento a.

Sejam A e B anéis. Vamos definir em A x B uma adição e uma multiplicação do seguinte modo: dados $(a_1, b_1), (a_2, b_2) \in \mathrm{A \times} B$, $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ e $(a_1, b_1).(a_2, b_2) = (a_1 a_2, b_1 b_2)$. Podemos verificar facilmente que A $x\ B$ munido das opera-

ções aqui definidas é também um anel. O zero deste anel é o par $(0,0)$. Se A e B têm identidades então A x B tem identidade, (1,1). O anel A x B é chamado produto direto dos anéis A e B.

Exemplo 17. Sejam A e B anéis com identidade. O conjunto $R = \{(0,b); b \in B\}$ é um subanel de A x B. Notemos que: $(0,0) \in R \Longrightarrow R \neq \phi$; se $(0,b_1),(0,b_2) \in R$ então $(0,b_1) - (0,b_2) = (0,b_1 - b_2) \in R$ e $(0,b_1).(0,b_1) = (0,b_1 b_2) \in R$. Notemos ainda que se A e B têm identidades então a identidade de A x B é $(1,1)$ enquanto que R tem identidade $(0,1)$. Ou seja, a identidade do subanel R é diferente da identidade do anel A x B.

Definição 10. Sejam A um anel comutativo com identidade e $a \in A\backslash\{0\}$, $a \notin A^*$. Dizemos que a é irredutível se, sempre que $a = bc$ com $b,c \in A$, temos que $b \in A^*$ ou $c \in A^*$. Dizemos que a é primo se, sempre que $a|bc$ com $b,c \in A$, temos que $a|b$ ou $a|c$.

Exemplo 18. Os primos dos inteiros já estudados é um exemplo de elementos irredutíveis e primos. Futuramente estudaremos anéis diferentes dos inteiros onde exibiremos outros exemplos. Apresentaremos um domínio no qual existem irredutíveis que não são primos.

RESUMO

Nesta aula, caro aluno, estudamos o conceito de anel, onde definimos, estabelecemos uma primeira classificação, apresentamos diversos exemplos e as proposições clássicas mais gerais da teoria.

ATIVIDADES

1. Sejam A um anel comutativo com identidade e $\cup(A)$ o conjunto de todos os elementos invertíveis de A. Mostre que $(\cup(A),\cdot)$ é um grupo.

2. Em $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, prove que $\bar{a}$ é invertível se, e somente se, $mdc(a,n) = 1$.

3. Identifique todos os divisores de zero de $\mathbb{Z}_6$ e de $\mathbb{Z}_{18}$.

4. Seja $\phi : \mathbb{Z}_+^* \longrightarrow \mathbb{Z}$, onde $\phi(n)$ é o número de inteiros m tais que $1 \leq m < n$ e $mdc(m,n) = 1$. Sejam $n \in \{2,3,4,\dots\}$ e $a \in \mathbb{Z}$ tais que $mdc(a,n) = 1$. Prove que $a^{\phi(n)} \equiv 1(mod\, p)$. Em particular, se $p \in \mathbb{Z}_+$ é primo e $p \nmid a$, temos $a^{p-1} \equiv 1(mod\, p)$. (Esta função é conhecida como função Phi de Euller e este último resultado como pequeno teorema de Fermat).

5. Se A é um anel comutativo e $, b \in A$ são divisores de zero, prove que ab também é divisor de zero.

6. Sejam $p \in \mathbb{Z}_+$ um primo e $A = \mathbb{Z}[p] = \{a + b\sqrt{p};\ a,b \in \mathbb{Z}\}$. Para $\alpha = a + b\sqrt{p}$ e $\beta = c + d\sqrt{p} \in A$, definamos as operações: $\alpha + \beta = (a + c) - (b + d)\sqrt{p}$ e $\alpha\beta = (ac + bd'p) + (bc + ad)\sqrt{p}$. Prove que $(A,+,\cdot)$ é um domínio.

7. Se $B_1, B_2, \dots, B_n, \dots$ é uma seqüência de subanéis de um anel A, prove que $B = \cap_{i=1}^{\infty} B_i$ também é um subanel de A.

8. Determine todos os subanéis de $\mathbb{Z}_6$.

9. Sejam A um anel e $Z(A) = \{b \in A;\ ab = ba,\ \forall a \in A\}$. Prove que $Z(A)$ é um subanel comutativo de A.

10. Prove que o conjunto N de todos os elementos nilpotentes de um anel comutativo com identidade A é um subanel. (Este subanel é chamado o nilradical de A).

COMENTÁRIO DAS ATIVIDADES

Na primeira atividade você deve ter usado a definição de elemento invertível e desenvolvido com facilidade.

Na segunda atividade, se você conseguiu resolver, deve ter usado o fato de que, $mdc(a,n) = 1$ se, e somente se, existem $b, m \in \mathbb{Z}$ tais que $ab + n = 1$.

Na terceira atividade a observação de que em $\mathbb{Z}_n$ um elemento é divisor de zero ou é invertível é útil!

Na quarta, você deve ter notado que $\cup\ (\mathbb{Z}_n)$ é um grupo finito de ordem $\phi(n)$.

Na quinta atividade, você deve ter usado a definição de divisor de zero e feito a atividade com facilidade.

Na sexta atividade, você, caro aluno, deve ter notado que as adição e multiplicação definidas são de fato operações de $\mathbb{Z}[\sqrt{\mathrm{p}}]\ x\ \mathbb{Z}[\sqrt{p}] \longrightarrow \mathbb{Z}[\sqrt{p}]$, que $0,1 \in \mathbb{Z}[\sqrt{p}]$ e que $\mathbb{Z}[\sqrt{p}] \subset \mathbb{Q}$, para concluir que $(\mathbb{Z}[\sqrt{p}], +, \cdot)$ goza de todas as propriedades de um domínio.

Na sétima atividade, você deve ter usado apenas a definição de subanel para fazer a prova proposta.

Na oitava, caro aluno, você deve ter notado que se $(B, +, \cdot)$ é um subanel de $(\mathbb{Z}_6, +, \cdot)$ então $(B, +)$ é um subgrupo do grupo finito $(\mathbb{Z}_6, +)$ e usado as propriedades aritméticas da ordem de $\mathbb{Z}_6$.

Na nona atividade, bastou usar com cuidado a definição de subanel para concluir a afirmação proposta.

Finalmente, na décima atividade, se $a, b \in N$ e $m, n \in \{1,2,3, \dots\}$ são tais que $a^m = b^n = 0$, para k suficientemente maior do que m e n, você deve ter usado a fórmula do binômio de Newton $(a - b)^k = \sum_{i=0}^{k} \binom{k}{i} a^{k-i}(-b)^i = \sum_{i=1}^{k} 0 = 0$ e concluído que $a - b \in N$. Que ab é nilpotente é simples: $(ab)^{mn} = (a^m)^n . (b^n)^{mk} = 0.0 = 0$.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).